# Scalable quantum based solutions for Blockchain Systems

Jelena Mišić, Vojislav B. Mišić
Toronto Metropolitan University, Toronto, ON, Canada

***Abstract*—We propose a scalable quantum architectures which can improve operation of Blockchain systems. We focus on permissioned blockchains with consensus derived from Practical Byzantine Fault Tolerance (PBFT). We propose multipartite entanglement quantum architectures that can perform PBFT. Further we develop quantum systems and algorithms that can support Proof of Stake (PoS) voting as well as voter election and voting in delegated Proof of Stake systems. Validating nodes within a cluster hold qubits entangled in multipartite structure. Due to maximally connected entanglement they jointly perform voting and calculate voting results. We propose algorithms that can track voter's behavior and detect collusion and voting centralization problem.**

## I. Introduction

In this paper, we propose to use a permissioned blockchain system formed by authorized nodes only; permissionless systems such as the one adopted by uPort [26] incur security risks due to the presence of non-authorized users and entities, and suffer from long periods of ledger inconsistency. We plan to redesign the consensus protocol and voting scheme of multi-cluster blockchain system using quantum technology. Basic consensus unit which will be Practical Byzantine fault tolerance (PBFT) [6] algorithm and more complex algorithms such as Proof of Stake (PoS) and Delegated Proof of Stake (DPoS) will have to be redesigned using quantum computing and communication primitives which offer better security and privacy compared to classical Internet communications channels. Namely, the no-cloning principle in quantum communications prevents interference by a third parties [30], [29]. Also behavior of entangled multipartite quantum structures can be exploited to prevent collusion and centralization in quantum voting protocols.

In this paper, we address challenges imposed to quantum blockchain systems through a Scalable Quantum Blockchain (SQ3) architecture, that supports record validation and insertion in a ledger, stored, and managed in an efficient, secure, and usable manner. To reduce latency and improve scalability, we split the blockchain network into multiple, hierarchically organized clusters. Each cluster executes its own consensus decision and sends it to a nearby cluster from the next higher tier. This process is repeated until the top cluster is reached. Top cluster executes the final consensus step, links the record into the blockchain and returns relevant information back to lower tier clusters, which then return data to proxy nodes which maintain copies of the blockchain. Design problems in SQ3 have following objectives:

1) How to implement basic quantum communication and orchestration of PBFT voting for a single voting committee? We will denote group of nodes involved in voting on a single record as a "cluster". Cluster should cover small geographical area since end-to-end latency limits the throughput of consensus algorithm,
2) How to achieve quantum based multiple-entry capability within single cluster that removes the dependence on a single leader which is a security risk and a performance bottleneck?
3) How to implement particular quantum based voting scheme and how to prevent collusion and centralization. We consider three consensus classes which include flat (no priority) voting using PBFT, PoS voting and DPoS algorithm The basic primitive of all these consensus protocols is quantum PBFT.
4) How to design quantum network controller for blockchain system which will distribute entanglements for each phase of election/voting.
5) How to interconnect clusters in a hierarchical manner in order to cover larger geographical area with reliable quantum and classical communications and with minimized latencies? Each quantum voting cluster processes records and passes them to higher voting levels until central cluster approves them.
6) How to coordinate voting and cluster interconnection for multiple parameters. For example, for human identity blockchain application one cluster may decide on one aspect of human identity while other may consider other aspects.

## II. Related work

Since this work addresses PoS and DPoS algorithms in permissioned blockchains that should be executed in combination of quantum environment and classical communications we will divide related work in two groups.

979-8-3315-2096-0/25/$31.00 ©2025 IEEE

### A. Quantum structures, networks and algorithms

According to the definition [30], multipartite entangled state is maximally connected if for any two qubits there exists a sequence of single qubit measurements on the other qubits that when performed leaves two qubits in an entangled state. Another desired feature is persistency of entanglement which corresponds to the minimum number of qubits that have to be measured in order to leave the resulting state as unentangled.

Maximally connected entangled multipartite states (MEMS) have been intensively researched in past decade.

$|GHZ\rangle$ multipartite entanglement structure has been proposed and analyzed in [11]. Application of $|GHZ\rangle$ family of states has been proven to be very useful in voting algorithms [8], [33], [31].

Graph based (aka cluster) state has been analyzed in [4], [28], [3]. Similar to graph states are $|C_n^3\rangle$ states proposed in [7].

Another significant $n$-multipartite entangled state is $W$ state, [10], [18]. Despite not being maximally connected, this state has inherent fairness, since only one node can measure its qubit as $|1\rangle$ [16].

Distribution of particles to nodes for an quantum structure resembling part of the Internet using a controller/coordinator node was proposed in [1] and [34]. End nodes further generate entanglements which are referred to as quantum links and communicate using them. However, fidelity of entanglement decays exponentially with distance. These problems are consequences of imperfections of quantum medium channel and quantum manipulations. To overcome problem of distance between end nodes quantum repeaters interconnect end nodes by merging entangled pairs over short distances into entanglement over long distances. This is done using entanglement swapping technique [23], [24].

Classical quantum protocols for voting, implemented using multipartite entanglement, were proposed in [14] proposing traveling and distributed ballots. Algorithm for surveying was proposed in [33] using phase shifts. Further improvements by adding scrutinizer and/or tally-node are proposed in [31], [35], [15] and [19]. However, all these algorithms address anonymity in voting which requires multiple teleportations and this gives them complexity that is not necessary for permissioned blockchain voting.

### B. PoS and DPoS algorithms in blockchains

In PoS systems, a voting node needs to purchase a stake, typically expressed in local tokens, to be allowed to vote for the block proposed for inclusion in the blockchain; the weight of the vote depends on node's stake [32]. Nodes are rewarded (i.e., their stake is increased) for truthful and successful voting, and penalized otherwise. PoS approach has been utilized for cryptocurrencies such as Ethereum after The Merge [5] and also in general consensus schemes applicable to a wide range of scenarios [9], [27].

Delegated proof of stake (DPoS) further enhances this approach by allowing voting nodes to periodically elect a committee of witnesses or super-representatives which then propose blocks and vote for them. Similar to PoS systems, witnesses are rewarded for proposing blocks that are accepted and appended to the shared blockchain ledger.

Some of the best known DPoS systems are EOS [12] which is based on the DPoS scheme proposed in [21]; Steem [13]; and TRON [32]. A common feature of those DPoS systems is the the operation of three functional layers:

- The lowest layer is comprised of all nodes, interconnected in a P2P network, which can purchase, hold, and transfer tokens in the form of local cryptocurrency.
- Tokens are also used to elect witnesses that propose and accept blocks to be included in the distributed ledger. A node that wants to become an elector must first buy voting power by committing (freezing) some amount of tokens, which are then allocated towards the election of witness candidates. Number of witness candidate nodes $C$ is a parameter of DPoS system: for example, $C = 127$ in TRON and $C = 30$ in Steem and EOSIO. In order to prevent centralization, the elector may need to divide its $K$ tokens among candidates it wishes to vote for.
- Election process chooses top $E$ nodes from $C$ candidates based on the number of received votes. The majority required is typically two-thirds of the number of nodes plus one. The elected nodes form the witness committee, which proposes and votes for blocks to include in the blockchain ledger.

One notable problem that most of the DPoS systems have not properly addressed is the centralization of decision power which has been identified in EOSIO [25], Steem [22], TRON [17] and a number of other public blockchains. Moreover, the line between PoS and DPoS systems is not clear; for example, witness candidates in TRON need to deposit some cryptocurrency before election in order to prevent malicious attacks, which allows witnesses with sufficient stake to incentivize voters to repeatedly elect them to the committee; they may collude to accept otherwise invalid data items.

Centralization, so far, has been countered by limiting the duration of voting power and randomization of the election and the proposer role, as is done in Ethereum 2.0 [5]. Ethereum 2.0 also limits the maximum stake that is taken into account in the voting process [2] and allows 'slashing,' i.e., removal of misbehaving delegates

from the committee.

## III. Multipartite entangled quantum states for voting

Each voting cluster must be comprised of maximally connected multipartite state [30] which enables computing within the cluster. Quantum computing within cluster includes election, voting and processing of data. First step towards MEMS is in entangling EPR pairs [31] using CNOT operation. Resulting four qubit structure has the form $|\eta_4\rangle = \frac{1}{2}(|0000\rangle + |0011\rangle + |1110\rangle + |1101\rangle)$. Since qubits in each position can have two different values two successive measurements in $Z$ (computational) or $X$ (Hadamard) basis will lead to EPR pair which proves maximal connectedness. However, if measurements are done in $Z$ basis two measurements will break the entanglement. As a consequence persistence of this state is 2. This state can be incremented in steps of two qubits.

Another important n-qubit MEMS structure is $|GHZ\rangle$ state [11] involving entanglement of $n$ quantum particles which is denoted as:

$$|GHZ_n\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}) \tag{1}$$

This MEMS stays maximally connected if individual qubits are measured in $X$ basis. However if single measurement is done in $Z$ basis whole state becomes un-entangled which leads to persistence of only 1.

Graph states containing $n$ qubits can be initialized by starting with state $|+\rangle$ for each qubit and by applying controlled phase operator $C_p = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11|$. First three graph (cluster) states are:

$$\begin{aligned}
|\phi_2\rangle &= \frac{1}{\sqrt{2}}(|+\rangle|0\rangle + |-\rangle|1\rangle) \qquad (2)\\
|\phi_3\rangle &= \frac{1}{\sqrt{2}}(|+\rangle|0\rangle|+\rangle + |-\rangle|1\rangle|-\rangle)\\
|\phi_4\rangle &= \frac{1}{\sqrt{2}}(|+\rangle|0\rangle|+\rangle|0\rangle + |+\rangle|0\rangle|-\rangle|1\rangle\\
&\quad + |-\rangle|1\rangle|-\rangle|0\rangle + |-\rangle|1\rangle|+\rangle|1\rangle)
\end{aligned}$$

By applying Hadamard transformation on $|+\rangle$ and $|-\rangle$, which is under umbrella of local operation and classical communication paradigm (LOCC) previous three states can be transformed to equivalent EPR state $|\Phi^+\rangle$, $|GHZ_3\rangle$ and $|\eta_4\rangle$ which are maximally connected. Adding more nodes in this manner will produce larger maximally connected cluster states. However, state $|\phi_n\rangle$, $n \geq 4$ is equivalent to $|\eta_n\rangle$, $n \geq 4$ state, and persistence of this kind of cluster state is $\lfloor \frac{n}{2} \rfloor$.

Recently, similar to graph state, n-qubit multipartite entangled structure $|C_n^3\rangle$ was analyzed in [7]. $|C_n^3\rangle$ is generated by preparing initial qubit particle $A_1$ in state $|0\rangle$. Further qubits are initialized in states $|-\rangle$ and entangled with sequence of controlled Pauli operators $CZ$ and $CNOT$ i.e.

$$|C_n^3\rangle = \prod_{j\in nbhd} (CNOT_{A_j} CZ_{A_j}) |-\rangle^{\otimes(n-1)} |0\rangle_{A_1}. \tag{3}$$

Orthogonal state $|\tilde{C}_n^3\rangle$ is formed with initial state $B_1 = |1\rangle$ and subsequent states $|+\rangle$. Entangling operations now have changed sequence i.e: $|\tilde{C}_n^3\rangle = \prod_{j\in nbhd}(CZ_{B_j} CNOT_{B_j}) |+\rangle^{\otimes n-1} |1\rangle_{B_1}$.
In order to show maximal connectedness for this structure we note that $|C_2^3\rangle = |\Phi^-\rangle$ and $|\tilde{C}_2^3\rangle = |\Psi^+\rangle$. Higher order states are built as:

$$|C_{n+1}^3\rangle = |C_n^3\rangle|0\rangle - |\tilde{C}_n^3\rangle|1\rangle \tag{4}$$

where $n+1$-st qubit can have any position in the entanglement. Therefore, by measuring one bit we are reducing structure to entanglement of lower order until we reach EPR pair. This proves maximal connectedness and also proves that persistency of $|C_n^3\rangle$ and $|\tilde{C}_n^3\rangle$ entanglements is $n-1$. Due to this property these MEMS are convenient for computing the sum of values stored at nodes within the structure.

Another significant $n$-multipartite entangled state is $|W\rangle$ state, which is denoted as:

$$|W_n\rangle = \frac{1}{\sqrt{n}}(|1000..0\rangle + |0100...0\rangle \ldots + |0000...1\rangle)$$

$|W\rangle$ state is not MEMS since measuring 1 at some qubit leaves other qubits in deterministic state $|0\rangle$; however measurement of $|0\rangle$ leaves entanglement of lower order which leads to persistence of entanglement equal to $n-1$.

### A. Computing consensus results within MEMS

We reiterate that PBFT consensus is executed in permissioned blockchain so node identities are known. Pre-prepare phase requires broadcast of the record so it will be done using classical communication combined with quantum protocol for starting the PBFT process. This protocol would require quantum broadcast of single qubit with contention resolution. Phases prepare and commit will be done mostly in quantum mode and only measurements will be communicated using classical channels.

*1) Computing consensus results with GHZ :* This protocol can be deployed for prepare, commit and delegate election phases. We first discuss how GHZ state can be used to communicate sum of weighted votes. For pure PBFT voting weights would be equal to 1 but in proof of stake (PoS) voting they may be larger than 1. GHZ state with $n$ spatially distributed qubits $|GHZ_n\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$ can be used to accumulate, and record (measure) phase changes tied to $|1\rangle$ bit relative to $|0\rangle$. This corresponds to rotations around z-axis of Bloch sphere.

Phase evolution on node $i$ is characterized with operator $U_i = |0\rangle\langle 0| + e^{i\alpha_i\theta_i}|1\rangle\langle 1|$ where $\alpha_i$ denotes the weight of reported phase and $\theta_i$ denotes phase measurement in some time period $T$. For PBFT voting each node will have vote weight $\alpha_i$ and basic phase shift will be $\theta$. Assuming that $\theta_{tot} = \sum_{i=1}^{n} \alpha_i\theta$ total system phase of MEMS then becomes:

$$\begin{aligned}|\Omega\rangle &= \prod_{i=1}^{i=n} U_i \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}) \\ &= \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + e^{i\theta_{tot}}|1\rangle^{\otimes n}) \end{aligned} \tag{5}$$

In order to estimate this total phase shift, Hadamard transformation has to be applied to each qubit [8]. After that each node has to measure its qubit in computational (Z) basis and report measurement using classical channel. If we assume that expression $|x| \in 0, 1$ represents Hamming weight (parity) of string $x$ this leads to following expression:

$$\begin{aligned}|\Omega\rangle &= \frac{1}{\sqrt{2^{n+1}}}((|0\rangle + |1\rangle)^{\otimes n} + e^{i\theta_{tot}}(|0\rangle - |1\rangle)^{\otimes n}) \\ &= \frac{1}{\sqrt{2^{n+1}}}\sum_{x\in 0,1}(1 + e^{i\theta_{tot}}(-1)^{|x|})|x_1, x_2 \dots x_n\rangle \\ |\Omega\rangle &= \frac{1}{\sqrt{2^{n+1}}}\sum_{x\in 0,1}(1 + \cos\theta_{tot}(-1)^{|x|} \\ &\quad + i\sin\theta_{tot}(-1)^{|x|})|x_1, x_2 \dots x_n\rangle \end{aligned} \tag{6}$$

In order to perform measurement for particular string $|x\rangle = |x_1, x_2, \dots x_n\rangle$ projector operator $Pr = |x_1, x_2, \dots x_n\rangle\langle x_1, x_2 \dots x_n|$ is selected. Probability of measuring value $|x\rangle$ is:

$$P_x = |Pr\,|x\rangle\,|^2 = \langle\Omega|\,Pr\,|\Omega\rangle$$

Further derivation leads to:

$$\begin{aligned}P_x &= \frac{1}{2^{n+1}}\left((1 + \cos\theta_{tot}(-1)^{|x|})^2 + \sin{\theta_{tot}}^2\right) \\ &= \frac{1}{2^n}(1 + \cos\theta_{tot}(-1)^{|x|}) \end{aligned} \tag{7}$$

Probability of measuring string with even parity is therefore equal to $P_{xe} = \frac{1}{2}(1 + \cos\theta_{tot})$ and probability of measuring odd parity is $P_{xo} = \frac{1}{2}(1 - \cos\theta_{tot})$. From a number of measurements, it is possible to estimate $P_{xe}$ and $\theta_{tot}$. Since, in permissioned blockchain network, maximum phase shift is known it is possible to publicly conclude whether $2/3 + 1$ consensus has been reached.

*2) MEMS computing consensus results with $|C_n^3\rangle$:* State $|C_n^3\rangle$ is recursively composed starting with states $|\Phi^-\rangle$ and $|\Psi^+\rangle$ so measuring relative phase shifts would be difficult. However, due to recursive composition of this state shown in expression 4 each qubit $i$ can be rotated by some angle $2\theta$ around $y$-axis of Bloch sphere. Rotation in clockwise direction as defined in [30] can be represented with matrix:

$$R(\theta) = \begin{vmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{vmatrix}$$

By applying single rotation operator to qubit $i$ we get:

$$\begin{aligned}|Rot_i\rangle &= R(\theta)(|C_{n-1}^3\rangle|0\rangle - |\tilde{C}_{n-1}^3\rangle|1\rangle) \\ &= |C_{n-1}^3\rangle(\cos\theta|0\rangle_i - \sin\theta|1\rangle_i) \\ &\quad + |\tilde{C}_n^3\rangle(\sin\theta|0\rangle_i + \cos\theta|1\rangle_i) \end{aligned}$$

If each node $k$ executes rotation of its qubit and includes weight factor $\alpha_k$ the total system state will experience total rotation of its $|0\rangle$ and $|1\rangle$ components as $\theta_{tot} = \sum_{k=1}^{n} \alpha_k\theta$. This can be measured at arbitrary node $i$ within MEMS as:

$$\begin{aligned}|\Omega\rangle &= |C_{n-1}^3\rangle(\cos\theta_{tot}|0\rangle_i - \sin\theta_{tot}|1\rangle_i) \\ &\quad + |\tilde{C}_n^3\rangle(\sin\theta_{tot}|0\rangle_i + \cos\theta_{tot}|1\rangle_i) \end{aligned}$$

Each node in state $|C_n^3\rangle$ can prepare its input for particular phase of PBFT protocol (prepare and commit). In this environment voting values can be communicated as rotations around $y$-axis of Bloch sphere. As in the previous case each node contributes with $\alpha_i\theta$ where $\alpha_i$ corresponds to the weight of the vote and $2\theta$ is basic rotation around $y$-axis.

### *B. Leader selection and contention resolution*

In the case of voting in the blockchain committee there is a question how to elect the leader node which will propose next block. First solution is to have semi-permanent leader which will propose the block. However, due to reliability and security issues it is better if this role is dynamically selected. While in classical blockchain P2P networks multiple access can be easily resolved using CSMA/CA technique for quantum systems it still represents a big challenge.

So far some techniques were dealing with contention detection and mitigation while others were dealing with contention prevention. For contention detection main approach is to use $|GHZ\rangle$ state within cluster of $n$ potential transmitters [8]. Designated node prepares a number of entangled states equal to the number of attempts to resolve contention and performs one negative phase rotation of whole $|GHZ\rangle$ state by angle proportional to the round of protocol. In transmission phase each transmitter rotates the phase with positive phase angle proportional to the round. After that each node performs Hadamard transformation, measures its qubit in computational $z$ basis and broadcasts the results. Parity of reported results determines if collision has occurred. Similar approach is reported in [20]. Another collision detection and mitigation approach [19] uses ring of EPR pairs allocated between the nodes and generalized CNOT operations within the ring in order to detect collision. Contention prevention based on $|W\rangle$

state was considered in [16]. In this scheme, before leader is elected each node measures its qubit and reports the result over classical channel. Due to inherent fairness of $|W\rangle$ leader selection follows uniform distribution.

However further research work is needed to improve contention resolution and design round robin and priority based leader selection using quantum algorithms. Priority should be based on history of voter's behavior.

This could be done by combining features of MEMS structure with $|W\rangle$ structure. For example, individual and total (virtual, honesty based) stake can be measured through $|C_n^3\rangle$ state and this can be used to create $|W\rangle$ with number of qubits proportional to the total stake. Qubits could be further distributed to voting nodes so that each node gets number of qubits proportional to its stake. In the arbitration phase nodes that have block for validation measure each of their qubits and report measurement results. Node that has measured $|1\rangle$ will take the role of leader and submit the block to witness nodes to vote. In this way priority differentiation is achieved since probability of measuring value 1 is proportional to $\frac{\alpha_i \theta}{\theta_{tot}}$. Node that has measured $|1\rangle$ announces this over classical broadcast channel. This resolves the tie among nodes with the same virtual stake in a fair uniformly distributed manner. Voting then proceeds using the quantum PBFT protocol.

### C. Quantum networks and repeaters

Since blockchain is P2P application over the quantum Internet it is also necessary to address problems related to MEMS computing over large distances. Quantum networks consist of end nodes and repeaters. End nodes generate initial entanglements of MEMS.

MEMS structures for blockchains have problems with fidelity of entanglements especially since they involve interactions and combinations of $|GHZ\rangle$, $|C^3\rangle$ and $|W\rangle$ structures. Swapping and purification in MEMS has to be done concurrently so that these structures are regenerated in minimal time.

In the context of blockchain operation over MEMS there is need for quantum network controller for the whole blockchain. Its task is to distribute entangled states for each blockchain state (election of witnesses, election of leader or voting). Currently controller designs are oblivious to the application [1],[34]. However, in blockchain setting controller needs to track operation of voter and leader elections and final voting. It is also in charge of repeaters within MEMS and decides about the routing, swapping and potentially purification. For example when $n$ sub-structures $|C_{n_i}^3\rangle$ need to be joined there should be one EPR pair $|\Phi^-\rangle$ between each of them. Those EPR pairs need to be concurrently swapped and if needed, purified.

### D. Centralization issues

To avoid centralization behavior of all nodes, voters' and leader's behaviour should be monitored. Monitoring should be done over long and short periods of time. Short time period is denoted as round and is equal to a multiple of voting cycles. For PoS scheme each voter starts the round with its current stake which has to be larger than minimum value. Stake changes during the round based on truthful voting, false voting and abstentions. If stake falls below the threshold node is excluded from the voting round. Such misbehaving node can buy additional stake but after prolonged time period.

For DPoS case, nodes first have to be elected and election result depends on node's behavior in previous voting rounds. However, wealthy electors can also use discretionary component in election. To mitigate this problem each voting node should start the round with same amount of virtual stake. That number evolves during round between minimum and maximum value. All nodes have the same initial, minimum and maximum virtual stake, but they may have different behavior in voting. They may have different probabilities of truthful voting, abstention or false voting. Successful and truthful voting leads to an increase in node's virtual stake, while abstention or non-truthful voting decreases it. As voting is conducted over MEMS, votes and virtual stakes should be made visible to each node in the system and should affect voter election for future round.

Stake for each node during the round can be tracked using MEMS structure where phase of each qubit represents node behaviour in one voting cycle. Namely, truthful, false voting and abstention correspond to different rotation angles either in $|GHZ\rangle$ or $|C^3\rangle$ structures. Measurement of this angle at the end of the round can be further used as input to election process for DPoS or to penalty wait for PoS structure. Elections can be also done using help of $|W\rangle$ structure where each candidate gets number of qubits proportional to its virtual stake (i.e. behavior in recent rounds). Candidate with highest number of qubits will have highest chance to being elected.

Leader which will propose next block should be selected based on the value of its current virtual stake (honesty) so that the node with highest virtual stake should be able to submit the block for approval.

### E. Multiparameter voting

Multiparameter voting would require a dedicated MEMS structure for voting and each parameter. It will also require relative ordering of weights given to each parameter. For example for blockchain for building identity score different validating authorities such as government, financial, education institutions and other may vote according to their data. Final results will be computed by top voting cluster and be represented as

a measure of trust placed in the given user identity. This could be done by having different quantum MEMS structures within cluster per authority. They will be further interconnected in higher level MEMS structure for final voting on identity.

## Conclusions and future work

In this paper we have discussed how election and voting algorithms in permissioned blockchain can be transformed for use over quantum Internet that consists of groups of multipartite entangled qubit structures interconnected using quantum links and quantum repeaters. We have shown that existence of maximally connected entangled multipartite structures as well as fair entangled structures as $|W\rangle$ allows distributed computing which corresponds to tracking of voter's behavior, witness election and voting on block inclusion in the case of blockchain. In future work we plan to develop quantum structures and algorithms to regulate dynamic multiple acces of nodes that have records for validation. Given large geographical coverage we plan to develop tiered quantum cluster architecture and methods of inter-cluster communication. Since clusters can decide on different aspects of records we need inter cluster communication that connects different aspects of users' records.

## References


[1] G. Avis, F. Rozpedek, and S. Wehner. Analysis of multipartite entanglement distribution using a central quantum-network node. *Physical Review A*, 107(1):012609, 2023.

[2] J. Beck. Rewards and penalties on Ethereum 2.0 [phase 0]., 2020. https://consensys.net/blog/codefi/rewards-and-penalties-on-ethereum-20-phase-0/.

[3] J.-C. Besse, K. Reuer, M. C. Collodo, A. Wulff, L. Wernli, A. Copetudo, D. Malz, P. Magnard, A. Akin, M. Gabureac, et al. Realizing a deterministic source of multipartite-entangled photonic qubits. *Nature communications*, 11(1):4877, 2020.

[4] H. J. Briegel and R. Raussendorf. Persistent entanglement in arrays of interacting particles. *Physical Review Letters*, 86(5):910, 2001.

[5] V. Buterin, D. Hernandez, T. Kamphefner, K. Pham, Z. Qiao, D. Ryan, J. Sin, Y. Wang, and Y. X. Zhang. Combining GHOST and Casper. arXiv preprint arXiv.2003.03052, May 2020.

[6] M. Castro and B. Liskov. Practical Byzantine fault tolerance. In *OSDI: Symposium on Operating Systems Design and Implementation*, New Orleans, LA, Feb. 1999.

[7] S.-Y. Chen, A. S. Cacciapuoti, X.-B. Chen, and M. Caleffi. Multipartite entanglement for the quantum internet. In *ICC 2023-IEEE International Conference on Communications*, pages 3504–3509. IEEE, 2023.

[8] M. Christandl and S. Wehner. Quantum anonymous transmissions. In B. Roy, editor, *Advances in Cryptology - ASIACRYPT 2005*, pages 217–235, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[9] P. Daian, R. Pass, and E. Shi. Snow white: Robustly reconfigurable consensus and applications to provably secure proof of stake. In *International Conference on Financial Cryptography and Data Security*, pages 23–41. Springer, 2019.

[10] E. D'Hondt and P. Panangaden. The computational power of the w and ghz states. *arXiv preprint quant-ph/0412177*, 2004.

[11] D. M. Greenberger, M. A. Horne, and A. Zeilinger. Going beyond Bell's theorem. In *Bell's theorem, quantum theory and conceptions of the universe*, pages 69–72. Springer, 1989.

[12] I. Grigg. EOS – an introduction. white paper. https://whitepaperdatabase. com/eos-whitepaper, 2017.

[13] B. Guidi, A. Michienzi, and L. Ricci. Steem blockchain: Mining the inner structure of the graph. *IEEE Access*, 8:210251–210266, November 2020.

[14] M. Hillery, M. Ziman, V. Bužek, and M. Bieliková. Towards quantum-based privacy and voting. *Physics Letters A*, 349(1-4):75–81, 2006.

[15] D. Horoshko and S. Kilin. Quantum anonymous voting with anonymity check. *Physics Letters A*, 375(8):1172–1175, 2011.

[16] J. Illiano, M. Viscardi, S. Koudia, M. Caleffi, and A. S. Cacciapuoti. Quantum internet: from medium access control to entanglement access control. In *2022 IEEE Globecom Workshops (GC Wkshps)*, pages 1329–1334. IEEE, 2022.

[17] S. E. Jeong. Centralized decentralization: Does voting matter? simple economics of the DPoS blockchain governance. Available at SSRN: http://dx.doi.org/10.2139/ssrn.3575654, April 2020.

[18] J. Joo, Y.-J. Park, S. Oh, and J. Kim. Quantum teleportation via a w state. *New Journal of Physics*, 5(1):136, 2003.

[19] E. T. Khabiboulline, J. S. Sandhu, M. U. Gambetta, M. D. Lukin, and J. Borregaard. Efficient quantum voting with information-theoretic security. *arXiv preprint arXiv:2112.14242*, 2021.

[20] A. Khan, U. Khalid, J. Ur Rehman, K. Lee, and H. Shin. Quantum anonymous collision detection for quantum networks. *EPJ Quantum Technology*, 8(1):27, 2021.

[21] D. Larimer. Delegated proof of stake (dpos), 2018. https://tokens-economy.gitbook.io/consensus/chain-based-proof-of-stake/delegated-proof-of-stake-dpos.

[22] C. Li and B. Palanisamy. Comparison of Decentralization in DPoS and PoW Blockchains. arXiv preprint arXiv.2002.02082, 2021.

[23] J. Li, M. Wang, K. Xue, R. Li, N. Yu, Q. Sun, and J. Lu. Fidelity-guaranteed entanglement routing in quantum networks. *IEEE Transactions on Communications*, 70(10):6748–6763, 2022.

[24] Z. Li, J. Li, K. Xue, D. S. Wei, R. Li, N. Yu, Q. Sun, and J. Lu. Swapping-based entanglement routing design for congestion mitigation in quantum networks. *IEEE Transactions on Network and Service Management*, 20(4):3999–4012, 2023.

[25] J. Liu, W. Zheng, D. Lu, J. Wu, and Z. Zheng. Understanding the Decentralization of DPoS: Perspectives From Data-Driven Analysis on EOSIO. arXiv preprint arXiv.2201.06187, 2022.

[26] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena. uPort: A platform for self-sovereign identity. white paper, 2017. https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf.

[27] S. Motepalli and H.-A. Jacobsen. Reward mechanism for blockchains using evolutionary game theory. arXiv preprint arXiv:2104.05849, 2021.

[28] M. A. Nielsen. Optical quantum computation using cluster states. *Physical review letters*, 93(4):040503, 2004.

[29] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Infrmation*. MIT Press, Inc., Boston, MA, 1st edition, 2010.

[30] E. G. Rieffel and W. H. Polak. *Quantum computing: A gentle introduction*. MIT press, 2011.

[31] J.-H. Tian, J.-Z. Zhang, and Y.-P. Li. A voting protocol based on the controlled quantum operation teleportation. *International Journal of Theoretical Physics*, 55:2303–2310, 2016.

[32] TRON DAO. TRON: Advanced decentralized blockchain platform. whitepaper version 2.0, TRON DAO, December 2018.

[33] J. A. Vaccaro, J. Spring, and A. Chefles. Quantum protocols for anonymous voting and surveying. *Physical Review A*, 75(1):012333, 2007.

[34] Z. Wang, J. Li, K. Xue, D. S. Wei, R. Li, N. Yu, Q. Sun, and J. Lu. An efficient scheduling scheme of swapping and purification operations for end-to-end entanglement distribution in quantum networks. *IEEE Transactions on Network Science and Engineering*, 2023.

[35] P. Xue and X. Zhang. A simple quantum voting scheme with multi-qubit entanglement. *Scientific reports*, 7(1):7586, 2017.